CLAIMS

We claim:

1. A Managed Security Server for use in a Secure Segment Communications Network, the Managed Security Server comprising:

   (a) a memory to store an address of at least one secure gateway device, wherein said secure gateway device is a member of the Secure Segment Communications Network; and

   (b) a processor for configuring said Secure Segment Communications Network by configuring the at least one secure gateway device.

2. The Managed Security Server of claim 1 wherein the Managed Security Server is a secure gateway device.

3. The Managed Security Server of claim 1 further comprising:
   wherein the memory stores a static public IP address, wherein the static public IP address is assigned to the Managed Security Server.

4. The Managed Security Server of claim 3 further comprising the at least one secure gateway device, the secure gateway device has a memory containing the static public IP address of the Managed Security Server.

5. The Managed Security Server of claim 1 wherein the address of the at least one secure gateway device is dynamically assigned.

6. The Managed Security Server of claim 1 further comprising:

wherein the input is additionally configured to receive a request for an address of a destination node, wherein the destination node is a part of said Secure Segment Communications Network.

7. The Managed Security Server of claim 6 wherein the request is tunneled and encrypted.

8. The Managed Security Server of claim 6 wherein said request is further comprised of an IP packet, wherein the IP packet has the virtual IP address in a IP address field and a public IP address encoded as a hardware address in a hardware address field.

9. The Managed Security Server of claim 6 further comprising:

an output configured to receive the request for an address from the second input, and to transmit the request for an address to the destination node.

10. The Managed Security Server of claim 9 wherein the destination node responds to the forwarded request for an address with an address response.

11. The Managed Security Server of claim 1 wherein a communication from a local area network to a second local area network is transferred through a wide area network by the at least one secure gateway devices through a tunnel.

12. The Managed Security Server of claim 1 further comprising:

wherein the output is also configured to output tunnel configuration information to the at least one secure gateway device.

13. The Managed Security Server of claim 1 further comprising

wherein the input is additionally configured to receive a transmission of data intended for a destination node.

14. The Managed Security Server of claim 13 further comprising

wherein the output is additionally configured to transmit the transmission of data to a secure gateway device that corresponds to the destination node.

15. The Managed Security Server of claim 1 further comprising:

wherein the output is additionally configured to transmit to the Secure Segment Communications Network IPSec configuration information.

16. The Managed Security Server of claim 1 further comprising:

wherein the output is additionally configured to transmit to the Secure Segment Communications Network IKE configuration information.

17. A method of managing a Secure Segment Communications Network, wherein the Secure Segment Communications Network is further comprised of a plurality of secure gateway devices, the method comprising the steps of:

(a) connecting the plurality of secure gateway devices to a communications network; and

(b) designating one of the plurality of secure gateway devices to be a Managed Security Server, wherein the Managed Security Server configures the Secure Segment Communications Network.

18. The method of claim 17 further comprising the step of:

(c) configuring the Secure Segment Communications Network at a second Managed Security Server secure gateway.

19. The method of claim 17 further comprising:

(c) assigning each secure gateway device of the plurality of secure gateway devices of step (a) an address that is independent of any other address on the network.

20. The method of claim 17 further comprising the step of:

(c) assigning the Managed Security Server a static public IP address.

21. The method of claim 20 further comprising the step of:

(d) storing at each secure gateway device of the plurality of secure gateway devices of step(a) the static public IP address of the Managed Security Server.

22. The method of claim 19 further comprising the step of

(d) dynamically assigning the address of step (c).

23. The method of claim 22 further comprising the step of:

(e) opening a registration channel from each of the secure gateway devices of the plurality of gateway devices of step (a) to the Managed Security Server; and

(f) conveying the dynamically assigned address of step(d) to the Managed Security Server.

24. The method of claim 23 further comprising the step of

(g) sending a request for an address of a destination node from a source node to the Managed Security Server, wherein the destination node is a part of said Secure Segment Communications Network.

25. The method of claim 24 wherein the request is tunneled and encrypted.

26. The method of claim 24 wherein the request is further comprised of an IP packet, wherein the IP packet has the virtual IP address in a IP address field and a public IP address encoded as a hardware address in a hardware address field.

27. The method of claim 24 further comprising the step of:

(h) forwarding the request for an address of a destination node of step (g) from the Managed Security Server to the destination node.

28. The method of claim 27 further comprising the step of:

(i) responding to the forwarded request for an address at the destination node of step (h) with an address response.

29. The method of claim 17 further comprising the step of:

(c) tunneling a communication from a local area network to a second local area network through the plurality of secure gateway devices.

30. The method of claim 17 further comprising the step of:

(c) providing tunnel configuration information from the Managed Security Server to the plurality of secure gateway devices.

31. The method of claim 17 further comprising the step of:

(c) receiving at the Managed Security Server a transmission of data intended for a destination node.

32. The method of claim 31 further comprising the step of:

(d) transmitting from the Managed Security Server the transmission of data of step (c) to a secure gateway device of the plurality of secure gateway devices that corresponds to the destination node.

33. The method of claim 17 further comprising the step of:

(c) receiving IPSec configuration information from the Managed Security Server for the Secure Segment Communications Network.

34. The method of claim 17 further comprising the step of:

(c) receiving IKE configuration information from the Managed Security Server for the Secure Segment Communications Network.

35. A source node for accessing a Secure Segment Communications Network, wherein said Secure Segment Communications Network is configured by a Managed Security Server, said source node comprising:

a first output configured to output a request for an address to a destination node to a Managed Security Server;

an input to receive an address from the Managed Security Server in response to the request for an address to a destination node; and

a second output configured to output data to a destination node according to the received address.

36. The source node of claim 35 further comprising:

wherein the Secure Segment Communications Network is configured by a second Managed Security Server in the event the Managed Security Server fails.

37. The source node of claim 35 further comprising:

wherein a secure gateway device of a plurality of secure gateway devices is assigned an address that is independent of any other address on the Secure Segment Communications Network.

38. The source node of claim 35 wherein the Managed Security Server has a static public IP address.

39. The source node of claim 38 wherein a secure gateway device of a plurality of secure gateway devices has a memory, wherein the memory contains the static public IP address of the Managed Security Server.

40. The source node of claim 37 wherein the address is dynamically assigned.

41. The source node of claim 40 wherein each of the secure gateway devices of the plurality of gateway devices opens a registration channel to the Managed Security Server to convey the dynamically assigned address.

42. The source node of claim 35 wherein the request is tunneled and encrypted.

43. The source node of claim 42 wherein the request is further comprised of an IP packet, wherein the IP packet has the virtual IP address in a IP address field and a public IP address encoded as a hardware address in a hardware address field.

44. The source node of claim 35 wherein the Managed Security Server receives the request for an address and forwards the request for an address to the destination node.

45. The source node of claim 44 wherein the destination node responds to the forwarded request for an address with an address response.

46. The source node of claim 35 wherein a communication from a local area network to a second local area network is transferred by a plurality of secure gateway devices through tunneling.

47. The source node of claim 35 wherein the Managed Security Server provides tunnel configuration information to a plurality of secure gateway devices.

48. The source node of claim 35 wherein the Secure Segment Communications Network receives IPSec configuration information from the Managed Security Server.

49. The source node of claim 35 wherein the Secure Segment Communications Network receives IKE configuration information from the Managed Security Server.

50. A method of managing a Secure Segment Communications Network, wherein the Secure Segment Communications Network is further comprised of a plurality of secure gateway devices, the method comprising the steps of:

(a) connecting the plurality of secure gateway devices to a communications network;

(b) designating one of the plurality of secure gateway devices to be a Managed Security Server, wherein the Managed Security Server configures the Secure Segment Communications Network;

(c) tunneling a broadcast or multicast transmission as a uni-cast transmission on a Internet to at least one secure gateway device with a known address, including the Managed Security Server; and

(d) transmitting said broadcast or multicast transmission from the Managed Security Server to a plurality of secure gateway devices with dynamically assigned addresses.